(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－115413

(43)公開日　平成７年(1995)５月２日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　9/00				
9/10				
9/12				
			Ｈ０４Ｌ　9/ 00　Ｚ	
		7304－5Ｋ	Ｈ０４Ｂ　7/ 26　１０９　Ｓ	

審査請求　有　請求項の数２　ＦＤ　(全７頁)　最終頁に続く

(21)出願番号　特願平5－282089

(22)出願日　平成５年(1993)10月18日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　白澤　進
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　蒲池　健一郎
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　友池　裕元
東京都港区芝五丁目７番１号　日本電気株式会社内

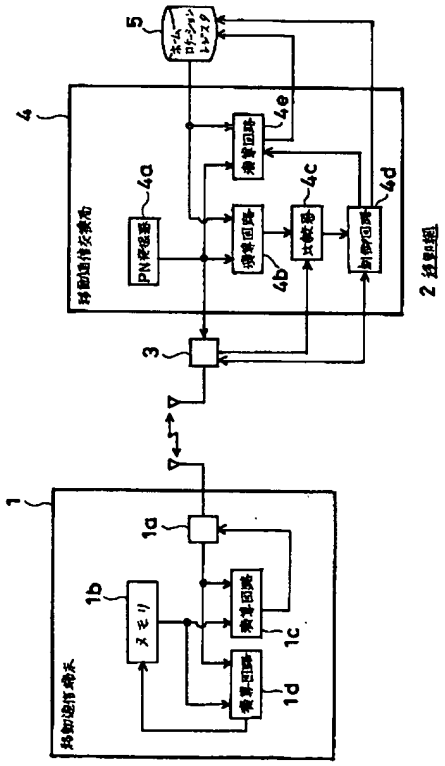
(74)代理人　弁理士　山川　政樹

(54)【発明の名称】　移動通信端末認証方式

(57)【要約】

【目的】　認証キーを端末と移動網間で伝送することなく更新させて移動通信システムの不正利用を防止する。

【構成】　ＰＮ発振器４ａから送信された乱数及びメモリ１ｂからの認証キーに基づく演算Ｆが演算回路１ｃで行われ、演算結果が移動網２に送信される。この演算結果と演算回路４ｂにて乱数及びホームロケーションレジスタ５からの認証キーに基づく演算Ｆが行われた結果とが比較器４ｃで比較される。比較結果が一致すると認証キー更新指示が制御回路４ｄから移動通信端末１に送信される。演算回路１ｄで乱数及び認証キーに基づく演算Ｇが行われ、新たな認証キーとしてメモリ１ｂに記憶される。演算回路４ｅにおいても同様に演算Ｇが行われてレジスタ５の認証キーが更新される。



1

【特許請求の範囲】

【請求項１】　移動通信システムの移動通信端末と移動網で同一の認証キーを記憶し、端末の正当性を確認する認証処理のための乱数を移動網から移動通信端末に送信する移動通信端末認証方式において、

受信した乱数及び記憶している認証キーに基づく第１の演算を行ってこの結果を送信し、認証キー更新指示を受信すると前記乱数及び認証キーに基づく第２の演算を行ってこの結果を新たな認証キーとして記憶する移動通信端末と、

前記乱数を生成して移動通信端末に送信すると共に前記乱数及び記憶している認証キーに基づく第１の演算を行い、この結果と移動通信端末から送信された結果が一致したときは、移動通信端末に認証キー更新指示を送信すると共に前記乱数及び認証キーに基づく第２の演算を行ってこの結果を新たな認証キーとして記憶する移動網とを有することを特徴とする移動通信端末認証方式。

【請求項２】　請求項１記載の移動通信端末認証方式において、

移動通信端末は、移動網と通信を行うための無線送受信機と、

認証キーを記憶するメモリと、

無線送受信機を介して受信した乱数及びメモリから出力された認証キーに基づく第１の演算を行いこの結果を無線送受信機に出力する第１の演算回路と、

無線送受信機を介して認証キー更新指示を受信すると前記乱数及び認証キーに基づく第２の演算を行いこの結果を新たな認証キーとしてメモリに記憶させる第２の演算回路とを有し、

移動網は、前記移動通信端末と通信を行うための無線基地局と、

認証キーを記憶するホームロケーションレジスタと、

交換接続を行う移動通信交換局とを有し、

この移動通信交換局は、前記乱数を生成して無線基地局に出力する発振器と、前記乱数及びホームロケーションレジスタから出力された認証キーに基づく第１の演算を行う第３の演算回路と、この第３の演算回路の結果と無線基地局を介して移動通信端末より受信した演算結果を比較する比較器と、この比較結果が一致したときは認証キー更新指示を無線基地局に出力する制御回路と、前記比較結果が一致したときは前記乱数及び認証キーに基づく第２の演算を行いこの結果を新たな認証キーとしてホームロケーションレジスタに記憶させる第４の演算回路とを備えることを特徴とする移動通信端末認証方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、移動通信システムにおいて、移動網との間で通信を行おうとする移動通信端末が移動網に登録された正当な端末であることを確認するための移動通信端末認証方式に関する。

2

【０００２】

【従来の技術】移動通信方式では、移動通信端末が無線回線で移動網と接続されているので、不正な移動通信端末による不正使用を防止し正当な端末に通信料の課金を行うためには、移動網に対して通信を要求する移動通信端末が移動網に登録された正当な端末であるかどうかを確認する認証処理が必要となる。

【０００３】図３は従来の移動通信端末認証方式を利用した移動通信システムのブロック図である。１１は移動通信端末、１１ａは移動網と通信を行うための無線送受信機、１１ｂは不正使用を防止するための暗証番号に相当する認証キーを記憶しているメモリ、１１ｃは認証キーと後述する乱数に基づき演算処理を行う演算回路である。

【０００４】また、１２は移動通信端末１１が契約している移動網、１３は移動通信端末１１と通信を行うための無線基地局、１４は例えば移動通信端末１１と他の固定網との交換接続を行う移動通信交換局、１４ａは認証処理のための乱数を通信の度に生成するＰＮ発振器、１４ｂはＰＮ発振器１４ａから出力された乱数と後述するホームロケーションレジスタに記憶されている認証キーに基づき演算処理を行う演算回路、１４ｃは演算回路１４ｂの結果と無線基地局１３を介して移動通信端末１１より受信した演算結果を比較する比較器、１４ｄは比較器１４ｃの結果に基づいて呼接続処理などを行う制御回路である。

【０００５】また、１５は例えば他の移動通信交換局（ホームメモリ局）に設置されたホームロケーションレジスタであり、移動通信端末１１の契約加入者情報、呼処理情報等を記憶しており、また移動通信端末１１のメモリ１１ｂに記憶されている認証キーと同一な認証キーを移動通信端末１１に対応づけて記憶している。そして、移動通信交換局１４は、移動通信端末１１からの通信の要求に対してホームロケーションレジスタ１５にアクセスして移動通信端末１１に関するサービス情報、呼処理情報、認証情報等を取得することができる。

【０００６】次に、このような移動通信システムにおいて移動通信端末１１が正当な端末かどうかを確認する認証処理の動作を説明する。まず、移動通信端末１１が移動網１２に対して発信要求を送信すると、無線基地局１３を介してこの発信要求を受信した移動通信交換局１４は、その内部のＰＮ発振器１４ａに乱数を発生させる。そして、この乱数は無線基地局１３から移動通信端末１１に送信される。

【０００７】次いで、移動通信端末１１内の無線送受信機１１ａは、移動網１２から送信された乱数を受信して演算回路１１ｃに出力する。演算回路１１ｃはこの乱数とメモリ１１ｂに記憶されている認証キーに基づいて演算を行い、無線送受信機１１ａはこの結果を移動網１２に送信する。

【０００８】一方、移動通信交換局１４内の演算回路１４ｂは、先にＰＮ発振器１４ａから出力された乱数とホームロケーションレジスタ１５に記憶されている移動通信端末１１の認証キーに基づき演算回路１１ｃと同一のアルゴリズムの演算を行う。そして、比較器１４ｃは、移動通信端末１１から送信された演算結果と演算回路１４ｂから出力された演算結果を比較する。

【０００９】この比較器１４ｃによる比較の結果２つの演算結果が一致すれば、制御回路１４ｄは、正当な端末と判定して移動通信端末１１と呼接続処理を行い、不一致であれば不正な端末と判定して呼接続処理を拒絶する。これで、認証処理が終了する。

【００１０】上記の移動通信端末認証方式は、記憶している同一の認証キーを同一の演算アルゴリズムを有する演算回路１１ｃ、１４ｂでそれぞれ演算処理してこれらの結果を移動網１２側で比較し、移動通信端末１１の正当性を判定するという認証方式である。しかし、移動通信端末１１と移動網１２で共有している認証キー、演算回路を不正にコピーした移動通信端末を作ったとすると、上記認証方式では移動通信端末１１の真偽を移動通信交換局１４で認識することができなくなる。

【００１１】そこで、特開平２－２２４４２５号公報で開示された移動通信方式は、通信の度ごとに次回使用する認証キーを送信し、移動網と移動通信端末双方で通信の度ごとに認証キーを更新して保持しておく認証方式となっている。この方式によれば認証キーを含めた移動通信端末がコピーされると、不正端末が通信を行った際に移動網側で認証キーが更新されて正規の端末の認証キーとの不一致が生じる。よって、次に正規の端末が通信を行う際に不一致となるので、正規の加入者は不正端末が存在することを早期に発見し、契約している移動網に申告し認証キーを再度設定することで一時的にこの不正端末を排除できる。

【００１２】しかし、この移動通信方式では次回使用する認証キーを移動網から移動通信端末に対して無線回線で送信するため、不正端末が移動網から送信された次回の認証キーを再度傍受することができれば認証キーを更新することができ、その不正端末は再度不正に移動通信サービスを受けることができてしまう。

【００１３】

【発明が解決しようとする課題】従来の移動通信端末認証方式は以上のようにして認証処理を行っていたので、記憶している同一の認証キーを演算処理してその結果を照合することにより端末の正当性を判定する認証方式では、認証キー及び演算回路をコピーした不正な端末が存在しても移動網側でその存在を認識できないという問題点があった。また、移動網と移動通信端末双方で通信の度ごとに認証キーを更新する認証方式では、次回使用する認証キーを移動網から端末に対して送信するので、一時的に不正端末を排除できても不正端末が次回の認証キーを傍受すると、その不正端末は再度移動通信サービスを受けることができてしまうという問題点があった。本発明は、上記課題を解決するために、端末と移動網で記憶している認証キーを伝送せずに更新させて移動通信システムの不正利用を防止することができる移動通信端末認証方式を提供することを目的とする。

【００１４】

【課題を解決するための手段】本発明は、受信した乱数及び記憶している認証キーに基づく第１の演算を行ってこの結果を送信し、認証キー更新指示を受信すると乱数及び認証キーに基づく第２の演算を行ってこの結果を新たな認証キーとして記憶する移動通信端末と、乱数を生成して移動通信端末に送信すると共に乱数及び記憶している認証キーに基づく第１の演算を行い、この結果と移動通信端末から送信された結果が一致したときは、移動通信端末に認証キー更新指示を送信すると共に乱数及び認証キーに基づく第２の演算を行ってこの結果を新たな認証キーとして記憶する移動網とを有するものである。

【００１５】また、移動通信端末は、移動網と通信を行うための無線送受信機と、認証キーを記憶するメモリと、無線送受信機を介して受信した乱数及びメモリから出力された認証キーに基づく第１の演算を行いこの結果を無線送受信機に出力する第１の演算回路と、無線送受信機を介して認証キー更新指示を受信すると乱数及び認証キーに基づく第２の演算を行いこの結果を新たな認証キーとしてメモリに記憶させる第２の演算回路とを有し、移動網は、移動通信端末と通信を行うための無線基地局と、認証キーを記憶するホームロケーションレジスタと、交換接続を行う移動通信交換局とを有し、この移動通信交換局は、乱数を生成して無線基地局に出力する発振器と、乱数及びホームロケーションレジスタから出力された認証キーに基づく第１の演算を行う第３の演算回路と、この第３の演算回路の結果と無線基地局を介して移動通信端末より受信した演算結果を比較する比較器と、この比較結果が一致したときは認証キー更新指示を無線基地局に出力する制御回路と、比較結果が一致したときは乱数及び認証キーに基づく第２の演算を行いこの結果を新たな認証キーとしてホームロケーションレジスタに記憶させる第４の演算回路とを備えるものである。

【００１６】

【作用】本発明によれば、移動網から乱数が送信され、移動通信端末にて受信した乱数及び記憶している認証キーに基づく第１の演算が行われて移動網に送信され、この演算結果と移動網の内部で乱数及び認証キーに基づく第１の演算が行われた結果とが比較される。そして、この比較結果が一致すると移動網から認証キー更新指示が送信され、移動通信端末にて乱数及び認証キーに基づく第２の演算が行われてこの結果が新たな認証キーとして記憶されると共に、移動網においても同様に第２の演算が行われて認証キーが更新される。

【００１７】また、無線基地局を介して発振器から乱数が送信され、受信した乱数及びメモリで記憶している認証キーに基づく第１の演算が第１の演算回路にて行われて無線送受信機を介して移動網に送信され、この演算結果と第３の演算回路にて乱数及びホームロケーションレジスタからの認証キーに基づく第１の演算が行われた結果とが比較器で比較される。そして、この比較結果が一致すると認証キー更新指示が制御回路から無線基地局を介して移動通信端末に送信され、第２の演算回路にて乱数及び認証キーに基づく第２の演算が行われてこの結果が新たな認証キーとしてメモリに記憶されると共に、第４の演算回路においても同様に第２の演算が行われてホームロケーションレジスタの認証キーが更新される。

【００１８】

【実施例】図１は本発明の１実施例を示す移動通信端末認証方式を利用した移動通信システムのブロック図、図２はこの移動通信端末認証方式における認証処理の手順を示す図である。

【００１９】図１において、１は移動通信端末、１ａは無線送受信機、１ｂは電源断時も内容を記憶している不揮発メモリであって認証キーを記憶しているメモリ、１ｃは図３の演算回路１１ｃと同様に受信した乱数とメモリ１ｂに記憶された認証キーに基づいて第１の演算を行う第１の演算回路、１ｄは無線送受信機１ａを介して認証キー更新指示を受信すると乱数及び認証キーに基づく第２の演算を行いこの結果を新たな認証キーとしてメモリ１ｂに記憶させる第２の演算回路である。

【００２０】また、３は無線基地局、４は移動通信交換局、４ａはＰＮ発振器、４ｂは演算回路１４ｂと同様にＰＮ発振器４ａから出力された乱数とホームロケーションレジスタに記憶されている認証キーに基づいて第１の演算を行う第３の演算回路、４ｃは第３の演算回路４ｂの結果と無線基地局３を介して移動通信端末１より受信した演算結果を比較する比較器である。

【００２１】また、４ｄは比較器４ｃによる比較結果が一致したときは認証キー更新指示を無線基地局３に出力して移動通信端末１に送信させる制御回路、４ｅは上記の比較結果が一致したときは乱数及び認証キーに基づく第２の演算を行いこの結果を新たな認証キーとしてホームロケーションレジスタに記憶させる第４の演算回路、５は図３の例と同様のホームロケーションレジスタである。

【００２２】図２において、Ｐ１ｎ、Ｐ２ｎはそれぞれホームロケーションレジスタ５、メモリ１ｂに記憶されている認証キー、Ｒｎ はＰＮ発振器４ａで生成された乱数、Ｃ１ｎ、Ｃ２ｎはそれぞれ第３の演算回路４ｂ、第１の演算回路１ｃによる第１の演算Ｆの結果、Ｐ１ｎ+１、Ｐ２ｎ+１はそれぞれ第４の演算回路４ｅ、第２の演算回路１ｄによる第２の演算Ｇの結果得られた新しい認証キーである。また、Ｆ（Ｐ１ｎ、Ｒｎ）は認証キーＰ１ｎと乱数Ｒｎ に基づく第１の演算Ｆを示し、Ｇ（Ｐ１ｎ、Ｒｎ）は同じく第２の演算Ｇを示す。

【００２３】次に、このような移動通信システムにおいて移動通信端末１が正当な端末かどうかを確認する認証処理の動作を説明する。まず、移動通信端末１からの発信要求を受信した移動通信交換局４は、制御回路４ｄによって移動通信端末１に関する呼処理情報を蓄積しているホームロケーションレジスタ５にアクセスし、発信要求の中に含まれる移動通信端末１の移動機番号（ＭＳＩ：Mobile Station Identity）で発信情報読み出しを要求する。

【００２４】そして、この要求に対する発信情報読み出し応答としてホームロケーションレジスタ５から出力された移動通信端末１の認証キーＰ１ｎ を受け取ると共に、ＰＮ発振器４ａに乱数Ｒｎ を発生させる。この乱数Ｒｎ は無線基地局３から移動通信端末１に送信される。また、演算回路４ｂは、ＰＮ発振器４ａから出力された乱数Ｒｎ とホームロケーションレジスタ５から読み出された移動通信端末１の認証キーＰ１ｎ に基づき演算Ｆを実行してこの結果Ｃ１ｎ を比較器４ｃに出力する。

【００２５】次に、移動通信端末１内の無線送受信機１ａは、移動網２から送信された乱数Ｒｎ を受信して演算回路１ｃに出力する。演算回路１ｃは、この乱数Ｒｎ とメモリ１ｂに記憶されている認証キーＰ２ｎ に基づき演算Ｆを実行してこの結果Ｃ２ｎ を無線送受信機１ａに出力する。この演算結果Ｃ２ｎ は無線送受信機１ａから移動網２に送信される。

【００２６】そして、移動通信交換局４内の比較器４ｃは、演算回路４ｂから出力された演算結果Ｃ１ｎ と移動通信端末１から送信され無線基地局３が受信した演算結果Ｃ２ｎ を比較し、移動通信端末１の正当性を判定する。このとき、移動通信端末１が正規の端末であればホームロケーションレジスタ５が記憶している認証キーＰ１ｎ と端末１が記憶している認証キーＰ２ｎ は同じはずであり、演算回路４ｂ、１ｃによる演算アルゴリズムも第１の演算Ｆで同一なので、演算結果Ｃ１ｎ とＣ２ｎ も等しいはずである。

【００２７】よって、移動通信交換局４内の制御回路４ｄは、比較器４ｃによる比較の結果２つの演算結果Ｃ１ｎ、Ｃ２ｎ が一致すれば正当な端末と判定し、無線基地局３に移動通信端末１に対して認証キー更新指示を送信させる。また、比較の結果が不一致であれば不正な端末と判定して認証がＮＧであったことを送信させる。

【００２８】ここまでの動作は図３の例と同様であるが、次に正当な端末と判定された移動通信端末１では、移動網２からの認証キー更新指示を受信することにより、以下のように認証キーＰ２ｎ の更新を行う。すなわち、演算回路１ｄは先の乱数Ｒｎ 及びメモリ１ｂに記憶されている認証キーＰ２ｎ に基づき演算Ｇを実行してこの結果Ｐ２ｎ+１ をメモリ１ｂに出力し、メモリ１ｂは記

憶している認証キーＰ２ｎ をこの新たに生成された認証キーＰ２ｎ+１ に更新する。

【００２９】一方、移動通信交換局４においても同様に演算回路４ｅが乱数Ｒｎ と認証キーＰ１ｎ に基づき演算Ｇを実行してこの結果Ｐ１ｎ+１ をホームロケーションレジスタ５に認証キー更新要求として出力する。そして、ホームロケーションレジスタ５は、記憶している認証キーＰ１ｎ をこの新たに生成された認証キーＰ１ｎ+１ に更新する。これで、認証処理が終了し、移動通信交換局４は移動通信端末１の発信要求に対する呼接続処理を行う。

【００３０】この認証方式では、ホームロケーションレジスタ５が記憶している認証キーＰ１ｎ と端末１内のメモリ１ｂが記憶している認証キーＰ２ｎ が同じで、演算回路４ｅ、１ｄによる演算アルゴリズムも第２の演算Ｇで同一なので、新たに生成された認証キーＰ１ｎ+１ 、Ｐ２ｎ+１ も同一となる。そして、次回の移動通信端末１に対する認証処理には今回の認証処理で更新されたこれらの認証キーＰ１ｎ+１ 、Ｐ２ｎ+１ が使用される。

【００３１】したがって、認証キーＰ１ｎ 、Ｐ２ｎ は通信の度に更新されるので、認証キー等が全く同等な不正端末を作ったとすると、この不正端末が通信を行った際には移動網２側で認証キーＰ１ｎ が更新され正規の端末１側の認証キーＰ２ｎ は更新されない。よって、次に正規の端末１が通信を行う際に認証キーが不一致となるので、正規の加入者は不正端末が存在することを早期に発見することができる。

【００３２】そして、無線回線でやり取りする主な情報は、ＰＮ発振器４ａで生成された通信の度ごとに変化する乱数Ｒｎ と演算回路１ｃによる演算結果Ｃ２ｎ であって、不正端末を作るのに必要となる認証キーが直接伝送されることはなく、また新しい認証キーは乱数Ｒｎ を用いた演算Ｇにより生成される。

【００３３】よって、ある時点で認証キー等が全く同等な端末を作ったとしても、その後の通信の際に移動網２から送信される乱数Ｒｎ を１度でも傍受し損なうと、正規の端末１の認証キーＰ２ｎ とホームロケーションレジスタ５の認証キーＰ１ｎ が更新されたにも関わらず、不正端末の認証キーは更新されないままとなり、それ以降不正端末の認証キーとホームロケーションレジスタ５の認証キーＰ１ｎ が一致することは極めて稀である。

【００３４】

【発明の効果】本発明によれば、移動通信端末と移動網で記憶している認証キーを通信の度に更新するので、認証キー等が全く同等な不正端末が存在しても、正規の端末が通信を行う際に認証キーの不一致が生じて不正端末が存在することを早期に発見することができる。また、認証キーを直接伝送せずに乱数を用いた第２の演算で認証キーを更新するので、乱数を傍受し損なうか又は不正端末の発覚による認証キーの再設定により、以後不正端末の認証キーと移動網の認証キーが一致することは極めて稀であり、不正端末による再度の不正な利用を防止することができる。

【００３５】また、移動通信端末を無線送受信機、メモリ、第１の演算回路、第２の演算回路から構成し、移動網を無線基地局、ホームロケーションレジスタ、並びに発振器、第３の演算回路、比較器、制御回路、及び第４の演算回路を有する移動通信交換局から構成することにより、移動通信端末と移動網で記憶している認証キーを直接伝送せずに、通信の度に乱数を用いた第２の演算で認証キーを更新させる移動通信端末認証方式を実現することができる。

【図面の簡単な説明】

【図１】本発明の１実施例を示す移動通信端末認証方式を利用した移動通信システムのブロック図である。

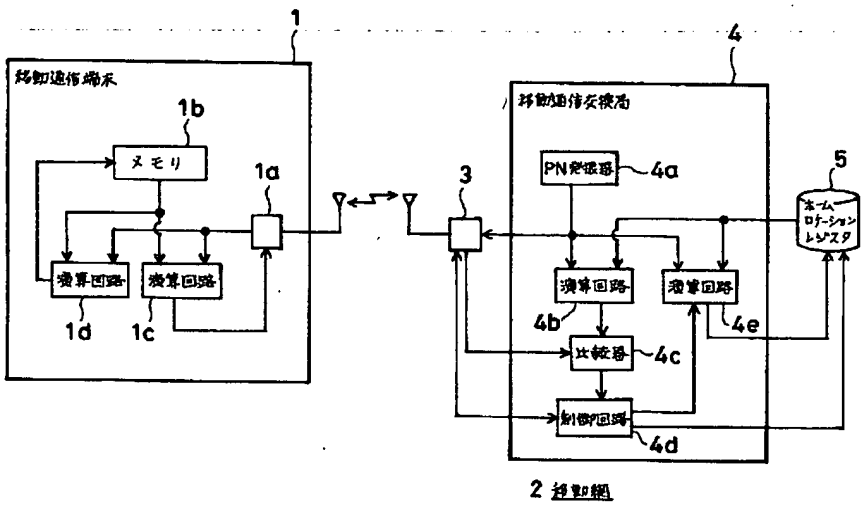
【図２】図１の移動通信端末認証方式における認証処理の手順を示す図である。

【図３】従来における移動通信端末認証方式を利用した移動通信システムのブロック図である。

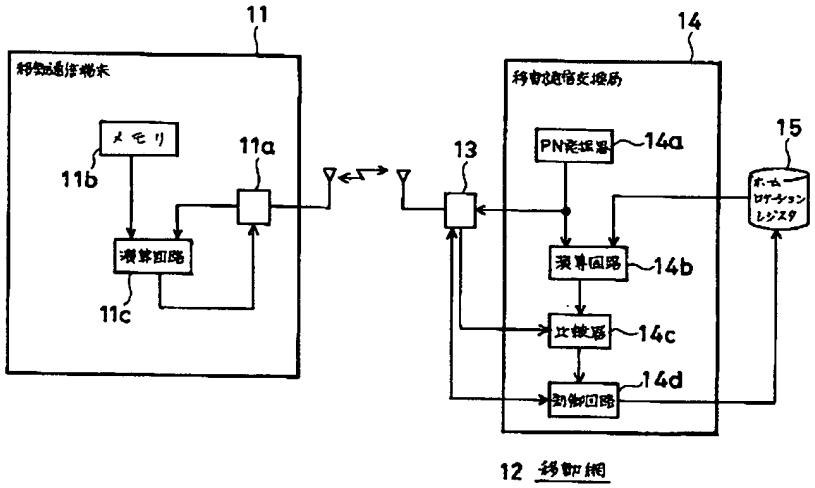
【符号の説明】

１　移動通信端末
１ａ　無線送受信機
１ｂ　メモリ
１ｃ　第１の演算回路
１ｄ　第２の演算回路
２　移動網
３　無線基地局
４　移動通信交換局
４ａ　ＰＮ発振器
４ｂ　第３の演算回路
４ｃ　比較器
４ｄ　制御回路
４ｅ　第４の演算回路
５　ホームロケーションレジスタ

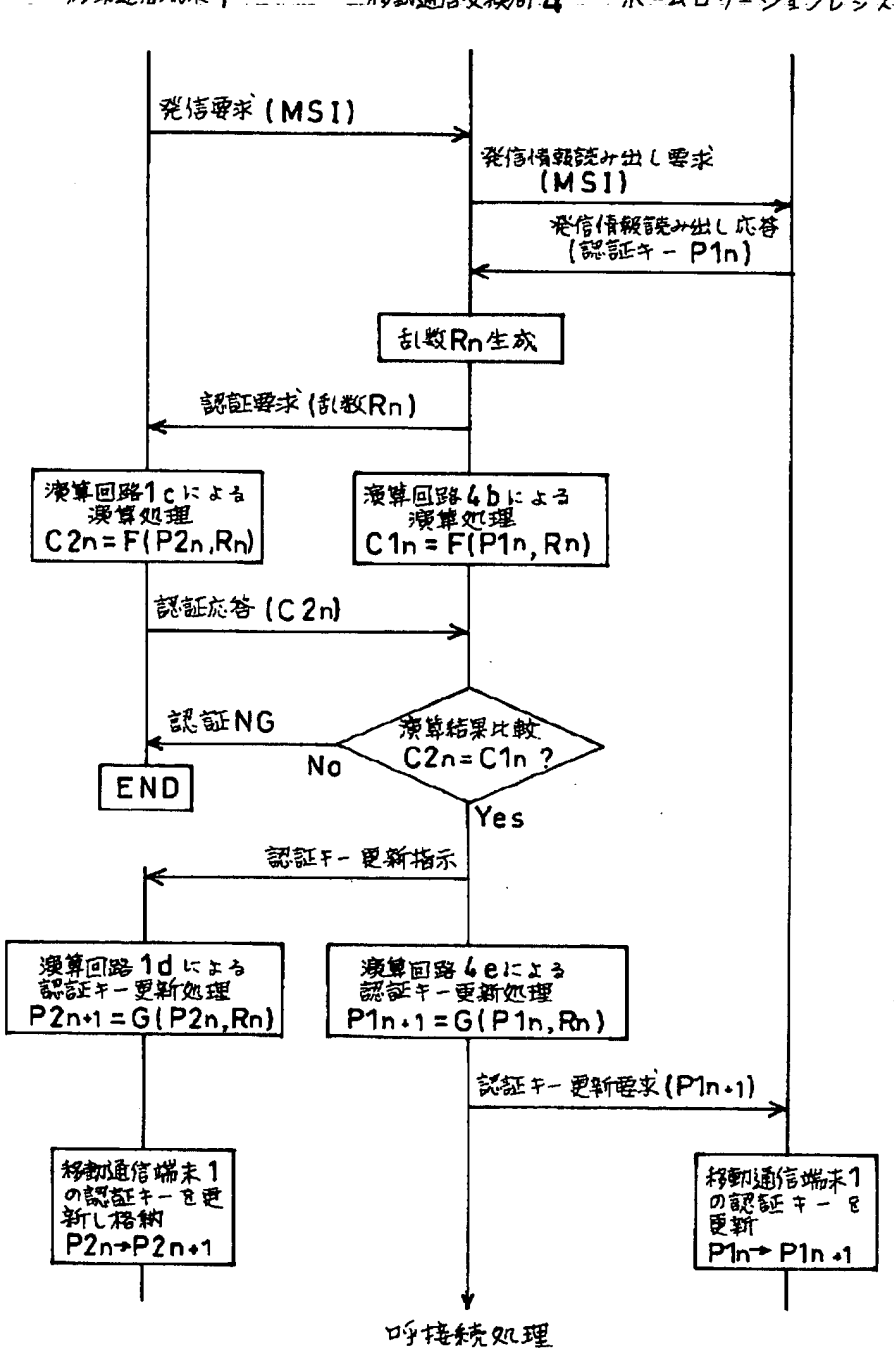
【図１】


1
移動通信端末
1b
メモリ
1a
演算回路
演算回路
1d
1c
3
4
移動通信交換局
PN発振器
4a
5
ホームロケーションレジスタ
演算回路
演算回路
4b
4e
比較器
4c
制御回路
4d
2 移動網

【図３】


11
移動通信端末
メモリ
11a
11b
演算回路
11c
13
14
移動通信交換局
PN発振器
14a
15
ホームロケーションレジスタ
演算回路
14b
比較器
14c
制御回路
14d
12 移動網

【図2】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
H04Q 7/38				